Zwolle

Raadsvoorstel

Datum 25 juni 2025

Onderwerp Robuuste Informatievoorziening
Versienummer 1

Portefeuillehouder Paul Guldemond

Samenvatting
We dragen zorg voor een robuuste informatievoorziening. Dit doen we aan de hand van een volwassenheidsmodel waarbij we achteruit kijken naar ons huidige niveau en vooruit kijken door het formuleren van een gewenst niveau. Op het gebied van informatiebeheer willen we een moderne, efficiënte en transparante informatiehuishouding realiseren die niet alleen voldoet aan wettelijke eisen maar ook de kwaliteit van dienst verlening en interne processen verbetert. Daarom werken we toe naar een stabiel volwassenheidsniveau II. Voor informatiebeveiliging geldt dat toewerken naar een stabiel niveau 3 waarmee we voldoen aan het BIO-normenkader. Werken aan de robuustheid van onze informatievoorzienig doen we niet alleen vanuit veiligheid en continuïteit maar ook vanuit vertrouwen; we willen dat inwoners ons kunnen vertrouwen met hun data.

Financiële gevolgen
Betreft doel 9.1.3 Informatievoorziening
Begroting wijzigen Nee
Budgetnummer

Bijlagen
1. Volwassenheid Informatiebeheer
2. Uitvoeringsplan Cyberbeveiligingswet (NIS2) Zwolle

Openbaarheid
☒ Openbaar
☐ Geheim

De raad wordt voorgesteld te besluiten om:
1. Kennis te nemen van het huidige volwassenheidsniveau op het gebied van informatiebeveiliging en informatiebeheer.
2. Het ambitieniveau op het gebied van informatiebeheer vast te stellen op niveau II en op het gebied van informatiebeveiliging niveau 3.

Datum 25 juni 2025

Inleiding

In de huidige digitale samenleving is informatiebeveiliging en -beheer een steeds grotere opgave voor de gemeente Zwolle. We vinden het belangrijk dat gegevens op een zorgvuldige en veilige manier worden behandeld en opgeslagen. Dit vereist niet alleen het naleven van wettelijke verplichtingen maar ook het implementeren van effectieve beveiligingsmaatregelen die onze bedrijfscontinuïteit waarborgen. In deze informatienota worden de huidige stand van zaken en de ambities op het gebied van informatiebeveiliging en -beheer uiteengezet. Omdat hier in grote mate sprake is van ketenafhankelijkheid betrekken we hierbij ook de samenwerking met SSC ONS, onze belangrijkste partner op het gebied van informatiebeheer en -veiligheid. Deze drie onderwerpen noemen we samen '*robuuste informatievoorziening'*.

In deze nota kijken we vooral naar hoe we het *nu* doen op deze thema's. Tegelijkertijd bevinden wij ons in een digitale transitie waarbij steeds meer ontwikkelingen in snel tempo op ons afkomen. De razendsnelle opkomst van AI of de verschillende informatiewetten uit Europa (digital decade) die op de gemeente Zwolle afkomen vragen ook om keuzes en bezinning. Separaat aan deze informatienota wordt daarom gewerkt aan het opstellen van een digitale strategie welke moet leiden tot overzicht en inzicht op het gebied van digitale keuzes. Deze Digitale Strategie Zwolle wordt in 2025 stap-voor-stap (agile) opgebouwd en in gebruik genomen. Het wordt niet een traditioneel document met een specifieke opleverdatum, maar continu (door)ontwikkeld zodat we koersvast en toch wendbaar kunnen sturen richting een onvoorspelbare digitale toekomst.

Voor informatiebeheer en -beveiliging geldt dat we ze voorzien van indicatoren waarmee we onze volwassenheid willen uitdrukken én een ambitie willen formuleren. Ook sluit deze ontwikkeling aan bij de ontwikkeling van een dashboard 'robuuste informatievoorziening' als onderdeel van onze nieuwe digitale strategie voor de organisatie. Deze nota beperkt zich tot de hoofdlijnen, meer gedetailleerde informatie is te vinden in onze uitvoeringsplannen (bijlage) en bevindingenrapportages van in- en externe auditoren (managementletter, ENSIA audit).

Kader

Kader stellende nota's rondom dit onderwerp zijn:

- Normenkader BIO/BIO2
- Wet Digitale Overheid (WDO)
- Wet Open Overheid (WOO)
- Archiefwet
- Informatiebeveiligingsbeleid (2022)

Beoogd effect

We dragen zorg voor robuuste informatievoorziening en we maken afspraken over het gewenste volwassenheidsniveau. Dit is gebaseerd op wat wij verantwoord vinden vanuit risico optiek en binnen de kaders van de wet, maar ook indachtig de alsmaar toenemende digitale dreiging en opgaven die zich aandienen. Zo ontwikkelen we ons naar volwassenheidsniveaus die passen bij de taken en opgaves waar we voor staan. Wij zijn ons ervan bewust dat de digitale transitie ons voor nieuwe uitdagingen stelt, met name als het gaat om de bescherming van onze meest waardevolle informatie ('kroonjuwelen').

Datum 25 juni 2025

Argumenten

1.1 Ons huidig volwassenheidsniveau op het gebied van informatiebeheer is bijna II

Op het gebied van informatiebeheer zijn de resultaten over 2024 nagenoeg gelijk aan de resultaten over 2023 zoals uw raad heeft kunnen lezen in het bevindingenverslag van de archiefinspecteur. Dat is niet verrassend. Op basis van het inspectierapport 2023 besloten we om eerst de randvoorwaarden te creëren om grip te krijgen op het informatiebeheer. De mate waarin we in control zijn als gemeente op het gebied van informatiebeheer is uit te drukken in een volwassenheidsmeting. Hiervoor gebruiken we een model van de rijksoverheid (volwassenheidsmeting informatiehuishouding). Dit model geeft vier verschillende niveaus van beheersing aan, variërend van ad hoc tot gemanaged. Door middel van een expertschatting hebben we bepaald op welk volwassenheidsniveau gemeente Zwolle zit. De uitgebreide onderbouwing hiervan is te vinden in bijlage 1.

Thema	Score	Oordeel
Hoofddoelen	1,75	Ad hoc
Thema 1: Professionals	1,75	Ad hoc
Thema 2: Volume en aard van informatie	1,67	Ad hoc
Thema 3: Informatiesystemen	2,5	Herhaalbaar
Thema 4: Bestuur en naleving	1,71	Ad hoc
Gemiddeld voor Zwolle	**1,88**	**Ad hoc**

LEGENDA

Niveau I: Ad hoc

Er wordt ad hoc en reactief gewerkt. Processen, procedures en beleid zijn niet gedefinieerd en verantwoordelijkheden zijn niet belegd. Ook de missie en visie ontbreken.

Niveau II: Herhaalbaar

Er ontstaat bewustwording voor het beschrijven van processen, procedures en beleid, maar worden alsnog ad hoc en inconsistent toegepast. Alleen de minimale vaardigheden zijn gedefinieerd. Training is mogelijk, maar wordt zonder achterliggend plan gedaan. Verantwoordelijkheden zijn wel beschreven.

Niveau III: Gedefinieerd

Er wordt gewerkt volgens de vereiste kaders. Processen, procedures en beleid worden gedefinieerd en uitgevoerd en verantwoordelijkheden en KPI's worden benoemd. Benodigde vaardigheden zijn gedefinieerd en trainingen vinden plaats op eigen initiatief. Strategie en visie zijn ontwikkeld en er zijn procedures ingericht om te evalueren wanneer systemen moeten worden veranderd.

Niveau IV: Gemanaged

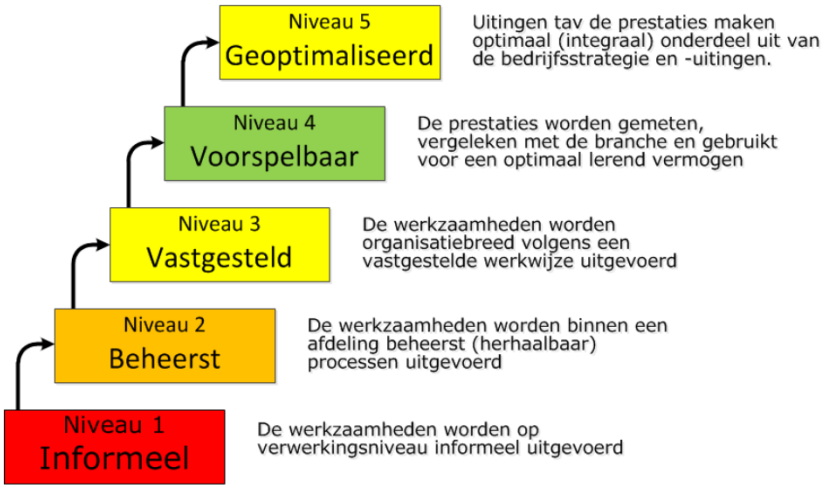
Er is sprake van "compliancy by design". Werkzaamheden zijn dus gekoppeld aan de visie en strategie van de organisatie. Processen en procedures zijn geïntegreerd in de organisatiestructuur. Er wordt proactief gewerkt aan het continu verbeteren van deze processen en procedures en er zijn procedures ingericht om actief in de gaten te houden wanneer systemen moeten worden veranderd. Trainingen worden juist structureel ingezet en kennisdeling wordt daarbij gestimuleerd. Ook wordt er actief data verzameld om het functioneren te evalueren en weer te verbeteren.

Er bestaan duidelijke wettelijke kaders waaraan de gemeente moet voldoen op het gebied van informatiebeheer. Indien dit onvoldoende gebeurt bestaat risico op verlies van informatie en kan er sprake zijn van toenemende kosten als gevolg van inefficiënte samenwerking of toegenomen operationele kosten in werkprocessen. Wat we hierbij voor de gemeente Zwolle van belang vinden is met name het maatschappelijk risico wat hierbij ontstaat als gevolg van afnemend vertrouwen in de

gemeente. We beschouwen daarom goed informatiebeheer niet alleen als wettelijke verplichting maar ook als essentieel voor het behoud van vertrouwen van onze inwoners en bescherming van onze democratische waarden.

1.2 Ons huidig volwassenheidsniveau op het gebied van informatiebeveiliging bevindt zich tussen de 2,2 en 2,5.

De Baseline Informatiebeveiliging Overheid (BIO) is het geldende normenkader voor alle gemeenten. Dit kader wordt onderdeel van de zorgplicht van NIS2 voor de overheid en krijgt daarmee ook een juridische waarde. Het voldoen aan de BIO en andere bestaande kaders voor informatiebeveiliging bij de overheid, is een belangrijk beginpunt. De NIS2-richtlijn brengt daarnaast enkele andere maatregelen met zich mee die nu nog geen onderdeel zijn van de BIO. De BIO kent vijf verschillende volwassenheidsniveaus. Deze worden enerzijds gebruikt om de mate van volwassenheid te meten maar kunnen ook gebruikt worden om te groeien in volwassenheid door het feitelijk verbeteren van de informatiebeveiliging. Niveau 3 wordt als minimum gezien om te kunnen stellen dat men zich aan de BIO houdt; op dit niveau is informatiebeveiliging bedrijfsbreed ingeregeld. Om volledig BIO compliant te zijn moet aan niveau 3 voldaan worden, alsmede een aantal eisen op niveau 4 en één op niveau 5.



Op het gebied van informatiebeveiliging is het van belang dat we onze informatiebeveiliging versterken en aanpassen aan de nieuwste wetgeving. In het licht van alle digitale ontwikkelingen is er sinds 2020 vanuit de Europese Unie dus gewerkt aan de *Network and Information Security (NIS2) directive*. Deze richtlijn is gericht op een verbetering van de digitale en economische weerbaarheid van Europese lidstaten. In Nederland wordt de NIS2-richtlijn geïmplementeerd in de vorm van de Cyberbeveiligingswet (Cbw). Deze nieuwe wet biedt niet alleen een kans om de digitale infrastructuur te verbeteren, maar vraagt ook om onze processen en verantwoordelijkheden opnieuw te evalueren. In het uitvoeringsplan cyberbeveiligingswet (bijlage 2) worden de implicaties van de nieuwe wetgeving uiteengezet, evenals de acties die nodig zijn om een robuuste en veilige digitale omgeving te creëren.

Op dit moment bevinden we ons nog op een volwassenheidsniveau tussen de 2,2 en 2,5 (expertschatting CISO gebaseerd op de nulmeting BIO). Hoewel de basis van onze informatiebeveiliging sterk is verbeterd ontbreekt nog een goede beheersings-systematiek om de implementatie van wet- en regelgeving gestructureerd uit te voeren en te monitoren. Daar waar het moet voldoen we aan de wettelijke eisen maar we kunnen niet stellen dat het huidige BIO normenkader al organisatiebreed ingevoerd is. De invoering van de cyberbeveiligingswet helpt én eist van ons dat we gerichte acties ondernemen op daarmee BIO-compliant te worden.

2.1 In de komende drie jaar willen we qua volwassenheid op het gebied van informatiebeheer toewerken naar een stabiel niveau II

We willen een moderne, efficiënte en transparante informatiehuishouding realiseren die niet alleen voldoet aan wettelijke eisen maar ook de kwaliteit van dienstverlening en interne processen verbetert. Dit vraagt naast duurzame opslag van data om professionalisering van onze systematische kwaliteitscontroles en -evaluaties. Uitgedrukt in een score betekent dit dat we streven naar een stabiel niveau II in 2027 uit het eerder genoemde volwassenheidsmodel. Deze ambitie vloeit voort en kan gerealiseerd worden door de middelen die eerder door u beschikbaar zijn gesteld voor informatiebeheer.

Een langetermijnstrategie anticipeert op verdere volwassenheidsgroei naar niveau III, vooral gedragen door de implementatie van een kwaliteitsmanagementsysteem. Hierbij is wel sprake van een onzekerheidsmarge door een wijziging in de archiefwet welke in behandeling is bij de eerste kamer. Door de VNG is aangegeven dat implementatie van deze wijziging (verwacht juli 2026) grote uitvoeringslasten voor gemeenten met zich meebrengt. In de begrotingscyclus 2027 verwachten wij hierover meer duidelijkheid en komen wij bij uw raad terug op het vervolg en de impact op onze ambitie qua volwassenheidsniveau.

Aanpak informatiebeheer

Informatie die duurzaam toegankelijk is; altijd vindbaar, beschikbaar, leesbaar, begrijpelijk, betrouwbaar én toekomstbestending blijft het hoofddoel. Voor iedereen die er recht op heeft en zo lang als het nodig is. Gezien de omvang van het informatiebeheervraagstuk is echter het *stapsgewijs* op orde brengen van onze (digitale) archieven noodzakelijk. De hoeveelheid digitale informatie is onvergelijkbaar veel groter dan in de tijd waarin we alleen met informatie op papier werkten en ook de diversiteit in soorten informatieobjecten is gegroeid. Er wordt steeds meer gewerkt in netwerken en op uiteenlopende platforms, zowel binnen de overheid als in interactie met burgers en ondernemers. De stroom aan informatie maakt de informatiehuishouding moeilijker te beheersen en op orde te houden. Dit vereist geavanceerde technieken voor datamanagement en -archivering waarbij we kiezen voor een risico gebaseerde aanpak die past bij de beschikbaar gestelde middelen. Door nieuw op te stellen informatiebeheerplannen af te stemmen op de eerder genoemde volwassenheidsniveaus creëren we eerst overzicht, sluiten we aan op de bevindingen van de archiefinspecteur en werken we methodisch aan verbetering van onze archieven. Dit geheel in lijn met één van onze digitale principes, *‘vertrouwen – Inwoners kunnen de gemeente vertrouwen met data en digitale technologie’.*

Er is voor deze aanpak van digitaal archiveren een richting gekozen die zowel door externen, het nationaal archief en interne stakeholders passend is bevonden. In brede zin stelt de archiefinspecteur dat Zwolle in de fase waarin het zich bevind de juiste focus heeft en de juiste onderkenning van de noodzaak in het archiveren van zowel data als documenten waarmee we vooroplopen op andere gemeenten. Zoals eerder met uw raad besproken past een ambitie om een ‘open archief’ te creëren nu nog niet bij de gekozen realisatiestrategie. Het *robuust* maken van het bestaande archief vraagt voor nu om keuzes binnen de huidige middelen zonder ruimte voor extra ambities. In het strategisch perspectief op de ontwikkeling van onze informatiehuishouding past deze ontwikkeling wel waarbij wij in de toekomst graag hierover het gesprek aan gaan met de raad.

2.2 In 2026 willen we qua volwassenheid op het gebied van informatiebeveiliging toewerken naar een stabiel niveau 3 waarmee we voldoen aan het BIO-normenkader.

De ambitie van de gemeente Zwolle is om in 2026 een robuuste digitale weerbaarheid te realiseren die voldoet aan de nieuwe eisen van de Cyberbeveiligingswet. Hiermee voldoen we aan het BIO-normenkader die onderdeel is van deze wet. Uitgedrukt in een waarde van het gekozen volwassenheidsmodel betekent dit dat we een structureel niveau 3 nastreven. Dit niveau is passend bij de dienstverlening en de huidige staat van onze informatievoorziening.

Het behalen van niveau 3 is een minimale vereiste om BIO-compliant te zijn. Gezien de almaar toenemende zwaarte als gevolg van de digitale transitie is volledig voldoen aan het normenkader geen eenvoudige opgave. Voor alle gemeentes geldt dat verbinden aan deze norm al een flinke opgave is waardoor de minister van Justitie en Veiligheid per kamerbrief heeft aangegeven dat de invoering van de cyberbeveiligingswet is uitgesteld tot het tweede kwartaal 2026. Daarmee loopt ons voorgestelde ambitieniveau parallel aan de landelijke inwerkingtreding.

Een hoger volwassenheidsniveau nastreven op het gebied van informatiebeveiliging is complex. Juist vanwege de snelheid van verandering in het domein en de groeiende wet- en regelgeving (van zowel het rijk als vanuit Europa) is compliant blijven al een uitdaging. Extra zorg besteden we wel aan onze ‘kroonjuwelen’, hard- en software die van essentieel belang is voor onze bedrijfscontinuïteit.

Aanpak informatiebeveiliging

Net als bij informatiebeheer geldt voor deze ambitie dat we kiezen voor een *risico gebaseerde* aanpak. De meest kritieke processen en gegevens krijgen prioriteit bij het nemen van beveiligingsmaatregelen. Uit het dreigingsbeeld informatiebeveiliging van de VNG blijkt dat gemeenten voor een onverminderd complex digitaal dreigingslandschap staan waardoor er risico’s zijn op ransomware of bijvoorbeeld incidenten bij leveranciers. Naast externe dreigingen kampen gemeenten met interne kwetsbaarheden. De menselijke factor blijkt een groter risico dan bewuste en gerichte aanvallen; onbewuste en onbedoelde acties van medewerkers zijn ook een primaire oorzaak van incidenten. Het feit dat medewerkers misleid kunnen worden door phishing is hier een voorbeeld van. Dit betekent dat informatiebeveiliging niet alleen gaat over het patchen van software en het beveiligen van netwerken, maar evenzeer over het menselijk gedrag en organisatiecultuur. Daarom werken we in meerdere sporen aan het verhogen van bewustzijn en kennis onder medewerkers en bestuur. In de komende drie jaar zal daarnaast de focus liggen op het verbeteren van de cyberweerbaarheid en het integreren van informatiebeveiliging in bredere gemeentelijke processen. Door gebruik te maken van nieuwe technologieën en samenwerkingsverbanden, willen we als gemeente Zwolle niet alleen voldoen aan wettelijke verplichtingen, maar ook het vertrouwen van burgers in onze digitale diensten versterken. Dit in overeenstemming met het digitale principe *‘vertrouwen – Inwoners kunnen de gemeente vertrouwen met data en digitale technologie’.*

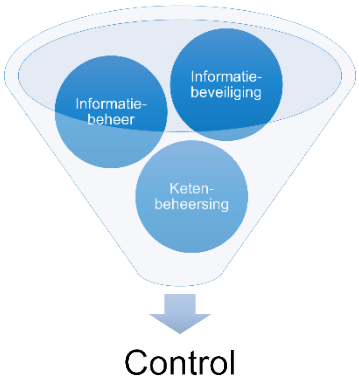
Ketensamenwerking

Bij zowel informatiebeheer als -beveiliging werken we samen in ketens om onze producten en diensten uit te laten voeren. Ook maken we in voorkomende situaties gebruik van externe ketenpartners voor de uitvoering van onze dienstverlening, bijvoorbeeld in het geval van SSC-ONS. Dit maakt beheersing van deze ketenprocessen tot een cruciale factor voor goede en efficiënte uitvoering van informatiebeheer en -beveiliging.

Datum 25 juni 2025

De gemeente Zwolle streeft naar continue verbetering (PDCA) van contract- en leveranciersmanagement om inzicht te krijgen in de effectiviteit van uitbestede dienstverlening en de verantwoordingsplicht van partners. Dit omvat het verkrijgen van Assurance-rapportages (zekerheid) om controle te krijgen over deze uitbestede processen, met een risico-gebaseerde aanpak en gezamenlijke KPI's. Hoewel de huidige IT-situatie een goede systeembeschikbaarheid en basale beveiliging kent, ontbreken structurele controles en rapportages wat het risico op lagere betrouwbaarheid vergroot. Er is behoefte aan meer aandacht voor IT-beheersmaatregelen zoals toegangsbeleid en wijzigingsbeheer. In de komende jaren zal Zwolle investeren in processen en tools die meer zicht bieden op de staat van informatievoorziening, waardoor compliance[1] en effectiviteit gewaarborgd worden. Externe samenwerking en evaluaties zullen bijdragen aan het realiseren van deze ambities binnen de context van een snel veranderende digitale omgeving.

Als gemene deler in bovenstaande vraagstukken geldt dat Zwolle op alle terreinen nog meer in controle wil komen. Meer controle op de risico's die we lopen op het gebied van informatiebeveiliging, maar ook meer regie kunnen voeren op onze uitbestede processen. Hiervoor zijn in 2024 al de nodige stappen gezet wat we ook terugzien in de recente bevindingen van onze accountant.



Deze ontwikkeling past bij de tijdgeest van digitale transformatie. Door de steeds sneller opeenvolgende mogelijkheden die ICT en data bieden worden we haast ingehaald door de techniek. Dit vraagt om herbezinning en strategisch positioneren. We streven niet naar een tien maar stellen ons tevreden als de basis *robuust* is. Door gelijktijdig onze digitale strategie Zwolle te ontwikkelen kijken we echter ook vooruit naar (andere) innovaties die op ons afkomen. Want ICT is niet alleen bedrijfsvoering maar manifesteert zich steeds duidelijker in al onze gemeentelijke opgaves.

In de komende jaren zal Zwolle investeren in processen en tools die ons meer zicht bieden over de staat van onze informatievoorziening om zo compliance en effectiviteit te waarborgen. We doen dit integraal waardoor risico's op het gebied van informatiebeveiliging en -archivering beheersbaar en transparant worden. Ook in onze samenwerking met SSC-ONS maken we dit expliciet waardoor we de gedachte van continu verbeteren willen versterken.

Externe samenwerking en onderzoeken (bijvoorbeeld van de rekenkamer) naar onze robuuste informatievoorziening helpen om verdere invulling te geven aan de ambities die we geformuleerd hebben. Onze digitale principes geven richting aan én vertellen ons hoe we invulling willen geven aan de digitale transitie. De snelheid waarmee nieuwe technieken ontwikkeld worden betekent echter ook dat we rekening hebben te houden met onzekerheid. Door de vernieuwende werkwijze van onze digitale strategie Zwolle, *waar robuuste informatievoorziening een onderdeel van is,* houden we hiermee rekening.

[1] De mate waarin we werken overeenkomstig wet- en regelgeving

Alternatieve mogelijkheden

Op het gebied van informatiebeheer geldt dat (gewijzigde) wetgeving voor een deel nog in behandeling is bij de 1e kamer. Dit bemoeilijkt het doorgroeien naar een volwassenheidsniveau III op de langere termijn. De ambitie voor informatiebeheer zou daarom gekoppeld kunnen worden aan de behandeling van deze wetswijziging en daarmee tijdelijk getemporiseerd worden. Echter; ook vanuit de gefaseerde invoering van de WOO worden eisen gesteld waardoor minimaal niveau II vereist is.

Het huidige volwassenheidsniveau op het gebied van informatiebeveiliging is niet conform het BIO normenkader. De geformuleerde ambities zijn in lijn met de wettelijke eisen die vanaf 2026 gesteld worden vanuit de cyberbeveiligingswet. Een lager niveau betekent daarom niet compliant zijn aan de BIO en achten wij daarom niet reëel. Hogere niveaus zijn gezien de vele opgaven waar Zwolle voor staat, de dynamiek binnen het vakgebied en het beschikbare budget niet haalbaar.

Maatschappelijk draagvlak & participatie

Inwoners hebben in toenemende mate zorgen over het gebruik van persoonsgegevens door de overheid. De digitale transformatie van de overheid vraagt om zorgvuldigheid bij de uitvoering. Het draagvlak bestaat namelijk vooral zolang de individuele inwoner er niet nadelig door wordt geraakt of er voordeel van heeft. Door helder te zijn over de robuustheid van onze informatievoorziening en de (on)mogelijkheden hiervan zijn we transparant over de wijze waarop gemeente Zwolle hiervoor zorgdraagt.

Communicatie

We vinden het belangrijk om vertrouwen te bevorderen en duidelijkheid te verschaffen over hoe de gemeente Zwolle omgaat met haar informatievoorziening. Door transparant te zijn over onze volwassenheid, ambitie en risico’s willen we uw raad betrekken en in staat stellen om haar controlerende functie uit te oefenen. Tegelijkertijd bestaat er een paradox: enerzijds is het van belang dat de gemeente open en toetsbaar is naar de buitenwereld toe, anderzijds mag de communicatie niet leiden tot het prijsgeven van kwetsbare interne processen of technische details die kwaadwillenden misbruik zouden kunnen laten maken van de gemeentelijke systemen. Daarom informeren we u op hoofdlijnen over dit onderwerp, waarbij nadere detaillering wordt aangebracht door andere onderzoeken zoals bijvoorbeeld door de rekenkamer of de IT-audit van onze accountant.

Financiën

Wat betreft onze uitgaven aan informatiebeveiliging geldt dat er geen vaste standaard is die voor alle gemeenten geldt. Gebruikelijk binnen gemeentes is dat een investering van minimaal 10% van de ICT-begroting in informatiebeveiliging een goede praktijk is. Dit helpt om een solide basis te leggen voor het beschermen van gegevens en systemen tegen bedreigingen. Inclusief de uitgaven die we in gezamenlijk verband via SSC-ONS doen zit Zwolle op 9%. Hoewel dit op het eerste gezicht zou kunnen suggereren dat er ruimte is voor aanvullende investeringen of dat er zelfs een tekort is zijn er op dit moment géén extra financiële middelen nodig om de gestelde ambitie om volwassenheidsniveau III (BIO-compliant) te bereiken. We vinden het belangrijk om eerst een robuuste basis neer te zetten. Voor een verdere doorgroei naar hogere niveaus zal afhankelijk van de door u gestelde ambitie in de begroting 2027 aanvullende middelen worden aangevraagd. We blijven de (landelijke) ontwikkelingen nauwlettend volgen en zullen u tijdig informeren over potentiële toekomstige financiële behoeften. We zullen hierbij uiteraard een gedegen onderbouwing presenteren, waarin de noodzaak en de verwachte resultaten helder uiteen worden gezet.

Datum 25 juni 2025

Risico's

Door de digitale transitie staat informatiebeveiliging en -beheer onder druk. Toenemende hoeveelheden data, applicaties en gebruikers worden gevolgd door alsmaar toenemende wet- en regelgeving vanuit het rijk en Europa. Om grip te houden en te voldoen aan deze eisen, hanteren wij daarom een risicogestuurde aanpak. Dit betekent dat we bewust keuzes maken op basis van de potentiële impact en waarschijnlijkheid van dreigingen. Daar waar het moet, geven we prioriteit aan het versterken van onze beveiliging en het verbeteren van ons informatiebeheer. Hierbij wordt steeds afgewogen tussen beschikbare middelen, wettelijke verplichtingen en de behoefte aan efficiënte dienstverlening. Door deze integrale benadering zorgen we ervoor dat zowel de belangen van onze inwoners als de continuïteit van de gemeentelijke operatie gewaarborgd blijven.

Vervolg

Na vaststelling van onze ambities gaan we verder met de uitvoeringsprogramma's op het gebied van informatiebeveiliging (cyberbeveiligingswet) en informatiebeheer. Daarnaast zetten we in op de invoering van een kwaliteitsmanagement methodiek om aantoonbaar richting onze auditoren in control te zijn. Tenslotte lanceren we een wendbare nieuwe (interne) Digitale Strategie Zwolle waarmee we bewuste keuzes willen maken wanneer het gaat over nieuwe digitale ontwikkelingen die op ons afkomen.

Openbaarheid

Openbaar

Burgemeester en wethouders van Zwolle,

burgemeester, Peter Snijders

secretaris, Dick Emmer